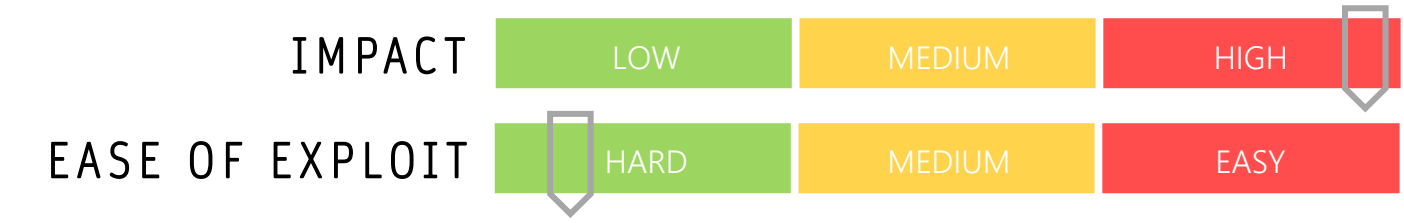
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00126

ANDROID SPYWARE MASQUERADES AS UPDATES

DATE ISSUED: 29th March 2021



OVERVIEW

Zimperium researchers have discovered a new spyware Remote Access Trojan (RAT) targeting Android devices that is capable of stealing extensive amounts of information off infected devices and masquerading as an update for a applications on third-party app stores.

BREAKDOWN

This new malware is not available on Google Play, but rather through applications sourced from third-party app stores and triggers whenever new information becomes available to exfiltrate – such as every time you receive a notification or commence any activity on the device. Posing as a system update, the RAT gives attackers almost full access to all information on the device across numerous messaging services, inspection of internet activities, clipboards, notifications, recording of audio and the ability to use the camera to take photos. Images, videos, contacts, call logs, device and connection information, photos and videos are all able to be sent back to the Command and Control (C2) server. The attackers went as far as to display a "searching for update" notification to hide their malicious activities and to reduce the risk of consuming too much bandwidth, only thumbnails of images are exfiltrated in further effort to avoid detection by the user.

REMEDIATION STEPS

- Only download applications from trusted sources, developers and app stores. Using third-party app stores heightens the risk of downloading malicious or Potentially Unwanted Applications (PUAs) as they do not have a stringent, thorough testing and qualification process.
- Monitor bandwidth usage.
- Install trusted mobile device endpoint protection software and conduct regular scans of your devices.
- Use Mobile Device Management Systems to control what applications your users are able to download.
- Connect BYOD devices to a separate internal network from the corporate network.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-android-malware-spies-on-you-while-posing-as-a-system-update/